Practical and ethical considerations on the use of cloud computing in accounting

Katherine Kinkela
Iona College

ABSTRACT

Cloud Computing promises cost cutting efficiencies to businesses and specifically their accounting departments through the use of third party vendors to store and process information. However this cloud computing innovation of storing and managing data off site also adds risk to the data security of a company. The Committee of Sponsoring Organizations (COSO), the Big Four accounting firms and other industry analysts have identified the benefits and concerns surrounding use of cloud technology and have prepared recommendations for companies who wish to utilize cloud computing on a formal or informal basis in their business operations. This paper will analyze the current advise on the risks of cloud computing in an effort to determine Best Practices for implementing use of and regulation of use of Cloud Computing within an organization.

Keywords: Accounting, Cloud Computing, Technology, COSO, Risk Management, Data Security

I. INTRODUCTION: POSITIVE ASPECTS OF CLOUD COMPUTING IN ACCOUNTING

Over the past several years, the technology enabling data storage outside of the computer has developed into usage of a cloud where computer software and data is housed and managed offsite. As with any type of outsourcing, cloud computing can offer tremendous efficiencies and cost cutting benefits. Because of the sensitive nature of accounting data, however, there is serious concern about the data security risks associated with allowing the third parties to manage the cloud. Section I part A of this paper will discuss what cloud computing is. Section I part B will identify the efficiencies and cost savings gained through cloud computing and will outline types of usage of cloud sources. Section I part C will discuss the recent report on cloud computing by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Finally, Section I part D will discuss recent guidance by the major accounting firms and accounting journals.

A. What is the Cloud?

According to COSO, "Cloud computing is a computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection. Depending on the cloud solution model an organization adopts, all or parts of the organization's hardware, software, and data might no longer reside on its own technology infrastructure. Instead, all of these resources may reside in a technology center shared with other organizations and managed by a third-party vendor." (COSO, 2012) In addition, according to Deloitte analyst Jean Griffin disruptive technologies, such as advanced analytics, social data and mobility are cloud based applications that will expand in the future. (Griffin, 2012)

As the above COSO definition of cloud computing suggests, the cloud may house data and software. The cloud configuration may be used on a project basis for sharing between locations. The cloud may hold entire databases or partial information. Because there are many types of cloud based applications, each applications should be reviewed by the organization before use to determine who has access and responsibility for maintaining the data and related software in the cloud.

Two major aspects of cloud computing are particularly notable. The first notable issue for adopters of cloud technology is that third party access to sensitive data requires a review of the third party data security policies and assurance of responsibility in the event of security breach. (KPMG, 2013) The second issue involves the fact that in the event of a program failure in the cloud the client may lack access or ability to remedy problems. (COSO, 2012) Use of third party software requires assurance of continuity of required business processes performed. (Hill & Wright, 2013) As discussed later communication and transparency between service provider and client are essential. The major accounting firms now provide assurance services to guide companies in this process of adopting and maintaining cloud computing resources. (Hill & Wright, 2013)

B. Efficiencies and Cost Savings Gained by Using Cloud Computing; Usage Strategies

Applications and Software capabilities are possible in the cloud. There is instant access to many programs. The Journal of Accountancy in a 2010 article, "Cloud Computing: what accountants need to know" identified uses for cloud based applications in audit confirmation, bill payment, customer relationship management, document management, financial statement preparation, payroll, sales and use tax and other uses. (Journal of Accountancy, 2010)

The use of a cloud computing system may give efficiencies of having an expert third party who can instantly adjust software instead of needing to send patches to upgrade software to the user. The cloud makes it easier to share data and related software because users can log in securely and remotely. There are benefits to having added storage space for data on the cloud; and the cloud may be used as an offsite backup for data in some cases.(COSO 2012)

The cost of the cloud-based technology is usually lower than traditional delivery methods. There are license fees and maintenance fees, however IT support is provided off site and can reduce infrastructure costs. Disruptive technologies and analytics can give smaller firms the opportunity to test these tools without committing to a full in house department. (Griffin 2012)

C. Recommendations by COSO

a. Background on COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), is dedicated to providing thought leadership through the development of comprehensive -frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by five organizations: American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives International (FEI), The Institute of Management Accountants (IMA) and The Institute of Internal Auditors (IIA).

b. COSO Thought Paper - Enterprise Risk Management for Cloud Computing

In June 2012, COSO released a thought paper entitled Enterprise Risk Management for Cloud Computing. The paper applies the COSO framework for ERM to the selection and implementation of cloud computing applications. The paper defines roles and responsibilities of the board of directors and Management of a corporation in the overall data security and business continuity processes.(COSO 2012)

D. Recommendations by Accounting Firms and journals

The major accounting firms and the accounting profession have responded to the increase in cloud based technology by providing an array of cloud based assurance services and guidance. The following is a sample of guidance provided by accounting firms and professional accounting organizations.

Professional accounting organizations such as the AICPA have identified cloud computing as a consideration in business operations. The Journal of Accountancy in a 2010 article, "Cloud Computing: what accountants need to know" identified uses for cloud based applications in audit confirmation, bill payment, customer relationship management, document management, financial statement preparation, payroll, sales and use tax and other uses. The Journal of Accountancy article recommended that reviews of infrastructure, software, personnel, procedures and data be evaluated before any cloud based applications are used in the accounting process. (Journal of Accountancy 2010)

Accounting firms such as Deloitte have turned this recommendation to review cloud based applications into an assurance business. Deloitte offers consulting at the outset of a cloud based vendor selection. In addition Deloitte offers services in "Cloud strategy, integration and migration." Consulting services may be used to develop and implement public, private, hybrid and community cloud environments. Vendor selection and system integration are also typically offered. (Callewalt, Robinson & Blattman, 2012)

These consulting services combine accounting and IT issues. They also assist in corporate governance issues, for example Deloitte provides "Data governance and policy management" services. Deloitte advises clients "As you work to shape the governance and policy frameworks needed to align to cloud services, we can help you establish policies, comply with regulations and enable effective data management and business capabilities integration." (Callewalt, Robinson & Blattman, 2012)

KPMG global consulting advises that analysis of the cloud related programs offered can help to set proper expectations on cloud use. Security related issues were identified as a primary concern of concern by businesses. Probably the largest segment of consulting lies in the data security area. Assurance groups review contracts to preserve client rights and to ensure that system requirements for data security are present before adoption and migration of sensitive data. (Hill & Wright, 2013)

Ernst and Young also identified business continuity issues of primary concern to adaprers of cloud technology. Inoperability of cloud systems may shut down business functions at critical times, and with no access to cloud contained technology, control as to recovery time for operating systems may not be possible. The E&Y consultants advised making sure that contracts with service providers require immediate repair actions and remedies for loss of business continuity. (Lemaire & Cara, 2012)

II. RISKS IN CLOUD COMPUTING

The security risks in cloud computing must be identified by the company in order to get a clear picture about the proper internal controls and related responses that a company should take to ensure the continued smooth operation of the company without fear of data disruption or compromise. (COSO, 2012) Section II part A discusses Cyber Security Issues. Section II part B provides risk assessment advice on cloud computing as

provided by COSO. Section II part C discusses risk identification and assessment issues in cloud computing as outlined by accounting firms.

A. Cyber Security

In order to understand the risks identifying types of data and related affected user groups is critical. Identifying risks to these groups is important. Risks include identity theft, business continuity issues and other factors.(COSO, 2012)

Risk assessment is a central objective to determine vulnerabilities in cyber security. Risk assessment should weight the benefits of the system with the magnitude and likelihood of potential risks.(COSO, 2012)

B. Risk Assessment Recommendations by COSO

Allowing a third party vendor access to sensitive data creates risks discussed by COSO in the Paper. The first concern discussed in the COSO paper is disruption of business processes where data is lost or compromised.(COSO, 2012)

The second concern discussed in the COSO paper are are Legal Risks abound by allowing a third party to have access to sensitive data and the power to manipulate or maintain that data. "Residing in the same risk ecosystem as the CSP and other tenants of the cloud: Legally, third-party cloud service providers and their customer organizations are distinct enterprises. However, if the CSP neglects or fails in its responsibilities, it could have legal liability implications for the CSP's customer organizations. But if a cloud customer organization fails in its responsibilities, it is less likely there would be any legal implications to the CSP."(COSO, 2012)

COSO next discusses that working through a third party requires communication and there is the danger of a lack of transparency. Finally there are Reliability and performance issues combined with contract issue about Vendor lock-in and lack of application portability or interoperability. (COSO, 2012)

C. Recommendations by Accounting Firms

KPMG identified the primary concerns associated with with data security. The key areas of concern are risk of intellectual property theft, data loss and privacy risk, general security risk, system availability and business continuity and legal and regulatory compliance including taxation. (Hill & Wright, 2013)

Ernst and Young identified that even merely transferring information over internet based systems increases vulnerabilities. In addition it is possible that different users within a cloud ay accidentally obtain access to sensitive data through a compromise in the cloud operating system. International laws concerning privacy may also apply if the service provider is not a US domestic company. (Lemaire & Cara, 2012)

Deloitte identifies the ease of implementation of cloud based products is balanced by availability, performance and security concerns. Deloitte examines the types of products offered via cloud technology as infrastructure as service, platform as service and software as service. Deloitte also identified the challenges of a changing legal landscape

that is evolving as the cloud based technology changes. (Callewalt, Robinson & Blattman, 2012)

III. BEST PRACTICES FOR MANAGING DATA AND THE CLOUD

Creating effective management of accounting data within the cloud requires proactive planning. Section III part A discusses developing best practices for managing data in the cloud including making sure that the Chief Information Officer or equivalent is aware of all the uses of cloud technology in the company. Section III part B discusses corporate governance and creation and Implementation of appropriate cloud usage policy. Section III part C discusses cyber insurance options.

A. Identifying possible uses/users of cloud technology

Corporations must understand that there are many programs that may be informally used to share information as well as comprehensive migrations of data to CSPs or third party service providers. Policies must be created for formal and informal uses of the cloud so that users understand the risks to data and business processes.(COSO, 2012)

COSO also discussed Cloud Computing in the paper from the perspective of Management Decisions. "Deciding whether to adopt cloud computing requires management to evaluate the internal environment – including the state of business operations, process standardization, IT costs, and the backlog of IT projects – along with the external environment – which includes laws and regulations and the competition's adoption of cloud computing. "(COSO, 2012)

COSO recommends that there should also be an understanding of the possibility of expansion and transferability options within the cloud system. The review process required by management will vary depending on the size of the corporation and the nature of the services provided by the cloud based service providers. (COSO, 2012)

B. Corporate Governance and Creation of Cloud Usage Policy

a. The Board of Directors has responsibility for oversight

Board of directors members should be aware of the corporate governance issues surrounding cloud computing. As identified by COSO, in a corporation cloud computing requires board of directors' oversight because use of the cloud is closely connected with the improvement and continuation of important business processes. The COSO White Paper on Cloud computing notes. "Given the opportunities cloud computing affords and the potential magnitude of its risk impact, cloud computing should be considered in the organization's overall governance activities and regarded as a topic warranting discussion and inquiry by an organization's board." (COSO, 2012)

As a part of routine corporate governance, the board must ensure that proper internal controls are used while implementing and maintaining cloud technology. It is the role of the board to determine the risk tolerances regarding use of cloud computing for

the organization and to review the work of management to ensure that risk tolerances are followed by management.(COSO, 2012)

The board should approve policies to cloud computing that will be communicated to employees. The policies on cloud computing should contemplate the array of potential uses for cloud based products and the scope of the projects.(COSO 2012)

b. Management must use Risk Assessment analysis prior to implementing use of cloud technology

While the board of directors will set the risk tolerances for the organization, management must implement the cloud based programs and monitor the programs through internal controls. COSO Notes: "In many cloud scenarios, the organization no longer has complete or direct control over technology and technology- related management processes. Management must determine if it has the risk appetite for the entire universe of potential events associated with a given cloud solution as some of these events extend beyond the organization's traditional borders and include some events that have an impact on the CSP (or CSPs) supporting the organization. "(COSO 2012)

For accountants, corporate data policy regarding cloud computing must be clearly annunciated and the internal controls necessary to use the cloud safely and effectively should be discussed. This implementation of the cloud and related controls should come as a part of the regular enterprise risk management of the corporation, COSO indicates: "The degree of adjustment required to an organization's existing ERM program in a cloud computing paradigm depends greatly on the business processes the cloud supports, the deployment model, the service delivery model, and the nature of the engaged CSP's risks and control environment." (COSO 2012)

Internal business policies relating to the cloud, therefore, must contemplate the scope and duration of the usage of the cloud and the contractual relationship between the company and the service provider.(COSO, 2012)

C. Cyber insurance policies

As an added protective measure many corporations are turning to cyber insurance policies that will provide assistance if there are process failures within the cloud. This insurance should be considered in coordination with the service provider contract. Cyber insurance policies are designed to cover losses in the event of a security breach. Policies can cover the cost of an investigation, communication and identity theft protection for at risk parties. (Griffin, 2012)

IV. RISK RESPONSES

At the time when a potential breach in data security is detected in the cloud, the company must decide what course of action to follow. Section IV part A outlines the investigation process made to determine the extent of the potential breach. Section IV part B discusses public disclosure of security breaches and the timing of disclosure so

that any affected parties are be notified of the breach as to prevent future harm. In addition, flaws in the system must be remedied to secure data in the future.

A. Investigation of possible data security breaches

Policies should be in place as to how to investigate if a breach is suggested. In addition, if the third party service providers are also investigating coordination is necessary between the company and the service providers. Contracts with service providers should include provisions that give access to the results of investigations and may allow the client company access to original documentation so that they may prepare their own investigation (Lemaire & Cara, 2012)

B. Public Disclosure and Remedial Actions

When the extent of the security breach has been determined the affected parties must be notified. Remedial actions within the company also need to be taken. The company must determine if the relationship with the service provider should be saved. There may be data transitioning issues. There may be business continuity issues. The scope of the problem should be identified. (Lemaire & Cara, 2012)

V. CONCLUSION

Cloud computing is now an accepted part of the array of technology available to accountants. Cloud computing can offer efficiency and cost cutting benefits. Before using cloud technology, however companies should understand the risks and security issues inherent in this new technology. By taking a systematic approach to risk assessment, including creating effective policies for cloud usage and a risk response plan, companies can take advantage of this new technology to increase operational efficiency.

REFERENCES

COSO (2012) Enterprise Risk Management for Cloud Computing. Washington D.C.:COSO.

Various Authors (2010) Cloud Computing: What Accountants Need to Know. North Carolina: Journal of Accountancy.

Drew, J. (2012) Heads in the Cloud. North Carolina: Journal of Accountancy.

Griffin, J. (2012) Managing Disruptive Technologies in the Cloud. New York: Deloitte.

Callewalt, P. & Robinson, P. & Blattman, P. (2012) Cloud Computing: Forecasting Change. New York: Deloitte.

Lemaire, O. & Cara, S. (2012) Cloud Computing: Issues and Challenges. New York: Ernst and Young.

Hill, S. & Wright, R. (2013) The Cloud Takes Shape. New York: KPMG.

KPMG (2013) Taking a Sober Look at Security. New York:KPMG.